UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/056,889	01/25/2002	Brian Swander	M1103.70145US00	1769

45840 7590 06/23/2006

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
FEDERAL RESERVE PLAZA
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/056,889	SWANDER ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 4/7/2006.

All objections and rejections not set forth below have been withdrawn.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 18 comprises the limitation *"wherein the steps of generating, determining and fragmenting are performed independently of performing any steps on the data packet corresponding to a transport layer protocol and/or a network layer protocol"*. The specification fails to provide proper antecedent basis for this limitation.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 18 and 19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. See above objection to the specification.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 18 and 19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 18, the phrase "and/or" renders the claim indefinite because it is unclear whether the limitation(s) qualified by the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim 19 is rejected by virtue of dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over IPSEC, "Minutes of IPSEC Working Group Meeting", in view of Kent et al. (Kent), "Fragmentation Considered Harmful".

Regarding claim 1, IPSEC discloses changes to the IKE protocol to support network transmission (i.e. NAT/Firewall traversal) (IPSEC, page 1, #1) and the testing of the traversal of IKE packets over NAT devices, thus the *generating and transmitting an IKE packet over a network* (IPSEC, page 4, lines 1-7). IPSEC discloses that changes to the IKE protocol (to solve the IKE/NAT problem) are needed as packet fragmentation adversely affects IKE packets (IPSEC, page 4, par. 2; "Revised ESP", pars. 2, 3). IPSEC discloses as a solution that packets should be fragmented above UDP, resulting in multiple UDP packets – each packet encapsulating a fragment from the above and highest layer [application layer] where the IKE protocol stack operates (for evidence of protocol stacks, Applicant's representative may refer to the applicant's admitted Prior Art, fig. 4). Thus, IPSEC discloses *fragmenting the IKE packet into a plurality of smaller*

packets and *transmitting each of the plurality of smaller packets over a network* (IPSEC, page 4, lines 1-7).

IPSEC discloses that IKE packets should be fragmented before the UDP layer. However, IPSEC does not disclose specifically methods packet fragmentation, such as conditions requiring fragmentation and that a packet fragment should have a proper packet header.

Kent et al. discloses principles for packet fragmentation. While Kent discusses these principals of packet fragmentation often in the context of the IP layer (Kent, pg. 75, par. 4), Kent further discloses that these fragmentation methods are to be applied in higher protocol layers as well. Upper level protocol layers should be cognizant of fragmentation issues, and should fragment or send smaller packet sizes if the it is known that a larger packet size will be fragmented at the IP layer (Kent et al., section 3, par. 4). For example, Kent discloses that an upper layer (i.e. TCP) should not send a large un-fragmented segment when it a lower layer (i.e. IP) will have to fragment it (Kent, pg. 79, pars. 3, 4).

Kent discloses that the packet fragmentation method consists of fragmenting a larger packet into a plurality of fragments. Each fragment is sent as a separate packet, with each of the plurality of smaller packets containing a properly formatted header according to the protocol (Kent et al., section 2.1).

It would have been obvious to one of ordinary skill in the art to employ the principles for packet fragmentation disclosed by Kent with the teachings of IPSEC requiring the fragmentation of IKE packets above the UDP layer. This would have been

obvious because one of ordinary skill in the art would have been motivated to practically implement packet fragmentation methods for the purpose of fragmenting IKE packets above the UDP layer as required by IPSEC, so that the packets would not be improperly fragmented at the IP layer. The combination of IPSEC and Kent discloses that fragmented packets each have a proper header, and thus, it would have been obvious to one of ordinary skill in the art to follow this teaching as required by the combination of IPSEC and Kent when fragmenting IKE messages before they are passed to the UDP layer.

Therefore, the combination of IPSEC and Kent et al. discloses:

determining whether a response to the IKE packet was received and *fragmenting the IKE packet into a plurality of smaller packets when a response is not received* (Kent et al., section 3.3). To avoid improper fragmentation at the IP layer, the combination of IPSEC and Kent et al. discloses that a transmitting host would choose whether to fragment an IKE packet using received acknowledgements ("a response") of successful packet transmission. If the host does not receive an acknowledgment ("a response") then it will have to fragment it's transmitted packets into smaller packets until it receives a successful transmission acknowledgment, and accordingly discovers the proper fragment length for transmitting packets.

Regarding claim 2, the combination of IPSEC and Kent et al. discloses:

wherein each header includes an identifier that may be used to associate the smaller packet with a corresponding IKE packet (Kent et al., section 2, par. 4, lines 1-8; section 2.1, par. 2)

Regarding claim 3, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination of IPSEC and Kent et al. discloses:

a User Datagram Protocol (UDP) stack that is capable of generating UDP data packets for transmission over a network,(IPSEC; page 4, lines 1-8). IPSEC discloses the generation of multiple UDP packets and the fragmentation of IKE packets above UDP (thus, a UDP stack) for network transmission;

an IKE protocol stack that generates IKE data packets that are subsequently processed by the UDP protocol stack (IPSEC; page 4, lines 1-8). IPSEC discloses the generation and fragmentation of IKE packets (thus an IKE stack). The packets pass from a layer above UDP to a layer below UDP, and are fragmented above the UDP layer.

and a fragmenter module that intercepts IKE data packets prior to being processed by to the UDP protocol stack and splits the IKE data packets into a plurality of smaller data packets that may be subsequently formatted by the UDP protocol stack (IPSEC, page 4, lines 1-8). IPSEC discloses fragmenting IKE packets (thus a fragmenter module) in a layer above the UDP layer (thus intercepting IKE packets prior to being processed by the UDP stack).

wherein, each of the plurality of smaller data packets includes a header formatted according to the IKE protocol (see rejection of claim 1).

Regarding claim 4, the combination of IPSEC and Kent et al. discloses:

generating an IKE data packet; intercepting the IKE data packet before it is passed to a subsequent network protocol stack (see rejection of claim 3);

determining a maximum size for fragments of an IKE data packet (Kent et al., section 3.3, par. 2).

dividing the IKE data packet into at least two smaller packets; and prepending a header to each smaller packet, wherein each header for each smaller packet includes an identifier that associates the smaller packet with its corresponding IKE data packet (see rejection of claim 1).

Regarding claim 5, the combination of IPSEC and Kent et al. discloses:

wherein the dividing step is performed such that the combined size of each smaller packet and prepended header will not exceed the maximum size (Kent et al., section 3.3, par. 2). The combination of IPSEC and Kent et al. discloses that the datagram size is chosen so that the fragmented packet (data + header) will not be fragmented ("will not exceed the maximum size").

Regarding claim 6, the combination of IPSEC and Kent et al. disclose:

receiving a plurality of fragments of an IKE data packet from a transmitting node,

wherein each fragment includes an identifier that associates each fragment with an IKE data packet ; and discarding all fragments that contain a first identifier if a predetermined number of fragments are received that contain a second identifier (Kent et al., section 2.4, par. 3).

Regarding claim 7, the combination of IPSEC and Kent et al. disclose:

wherein the step of discarding all fragments that contain a first identifier is performed when at least one fragment is received that contains a second identifier (Kent et al., section 2.4, par. 3).

Regarding claim 8, the combination of IPSEC and Kent et al. disclose:

determining whether all fragments that are associated with an IKE data packet have been received, and sending a no acknowledgment (NAK) message to the transmitting node when at least one fragment has not been received (Kent et al., section 3.3.3). A receiving host is disclosed as making a determination as to whether all fragments associated with an IKE packet has been received. The receiving host will convey a "Time exceeded" message ("NAK") to the transmitting host when at least one fragment has not arrived, indicating to the transmitting host that it has not received all the fragments.

Regarding claim 9, the combination of IPSEC and Kent et al. disclose:

determining the total size of all fragments that contain the same identifier and discarding said fragments when the total size exceeds a predetermined limit (Kent et al., section 2.4, par. 3).

Regarding claim 10, the combination of IPSEC and Kent et al. does not disclose *wherein the predetermined limit is 64 kilobytes.* This, however, would have been obvious to one of ordinary skill in the art to set a predetermined limit of 64 kilobytes as the total size of all possible fragments. As evidenced by the "Glossary for the Linux FreeS/WAN project" – (definition for DoS), this would have been obvious to one of ordinary skill in the art because the standardized size limit of an IP packet is 64 kilobytes, and a failure to discard illegitimate packets when the size exceeds the standard limit would result in denial of service attacks.

Regarding claim 11, it is rejected, at least, for the same reasons provided for the rejection of claims 1 and 2.

Regarding claim 12, the combination of IPSEC and Kent et al. disclose:

further comprising means for determining the capability of the receiver node for receiving fragmented packets (Kent et al., section 3.3, par. 2).

Regarding claims 13, 14, and 15 they are rejected, at least, for the same reasons as claims 1 and 2.

Regarding claim 16, the combination of IPSEC and Kent et al. disclose: *wherein the plurality of smaller packets contain the same information as that contained within the original IKE packet* (Kent et al., section 2.4, par. 3, section 2.1).

Regarding claim 17, the combination of IPSEC and Kent et al. disclose: *wherein at least one of the plurality of smaller packets contains the header formatted according to the IKE protocol* (Kent et al., section 2.1). As disclosed by the combination of IPSEC and Kent et al., fragmentation involves fragmenting the original packet into smaller packets, each containing the protocol and header fields of the original packet.

Regarding claim 18, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination of IPSEC and Kent discloses: *wherein the steps of generating, determining and fragmenting are performed independently of performing any steps on the data packet corresponding to a transport layer protocol and/or a network layer protocol* (IPSEC, page 4, lines 6-8). The combination of IPSEC and Kent discloses generating and fragmentation (accordingly determination to fragment) as occurring before the lower protocol layers.

Regarding claim 19, the combination of IPSEC and Kent et al. disclose:

wherein the step of determining whether fragmentation is necessary is not based exclusively on the size of the data packet (Kent et al., section 2, par. 3, lines 1-6; section 3, pars. 1 – 6). The combination of IPSEC and Kent et al. disclose the step of determining whether fragmentation is necessary is based upon the size of the data packet + overhead size.

Regarding claims 20 and 21, they are rejected, at least, for the same reasons as claim 1, and further because the combination of IPSEC and Kent et al. disclose:

fragmenting the packet into a plurality of fragments using a code module that does not implement the TCP, UDP or IP protocols before the packet is processed by a code module that does implement the TCP, UDP or IP protocols (IPSEC; page 4, lines 1-8; Kent et al., section 3). The combination of IPSEC and Kent et al. disclose the fragmentation of IKE packets above the UDP layer - this would include TCP (parallel to UDP) and IP (below UDP). The fragmentation is computer based and therefore inherently performed by some type of module for instructing a computer ("code module").

comprising including an identifier that identifies the data packet in eah packet fragment (see rejection of claim 2); *and transmitting the packet fragments over a network* (see rejection of claim 1).

Regarding claim 22, the combination of IPSEC and Kent et al. disclose:

receiving a plurality of data packets containing Internet Key Exchange (IKE) information, wherein the packets were transmitted from a transmitting node in a order that can be determined from information contained within the received data packets (Kent et al.; section 2.1, par. 3; section 2.4, par. 3);

determining from information contained within the received data packets whether any of the received packets have been received in an order that differs from the order in which the packets were transmitted from the transmitting node (Kent et al.; section 2.1, par. 3; section 2.4, par. 3);

and discarding at least certain of the received packets when a predetermined number of out of order packets have been received (Kent et al.; section 2.1, par. 3; section 2.4, par. 3).

Regarding claim 23, the combination of IPSEC and Kent et al. do not specifically disclose the *step of sending a message to the transmitting node that out of order packets have been received.* The combination does disclose the sending of a message to the transmitting node so as to acknowledge that the packets have been received in order (Kent et al.; section 2.1, par. 3; section 2.4, par. 3). It would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to also send a message acknowledging that the packets were not received in order. This would have been obvious because one of ordinary skill in the art would have been motivated to alert the system when transmission errors occur, so as to facilitate the operation of the system.

Response to Arguments

Applicant's arguments filed 4/7/06 have been fully considered but they are not persuasive.

Applicant's arguments with respect to claim 3 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's representative argues primarily that:

(i) The combination of IPSEC and Kent is Improper because:

However, not only does Kent not disclose IP layer fragmentation at upper level protocol layers, but it discloses the very opposite, that fragmentation should be performed at the IP datagram layer, i.e., the network layer (i.e., layer 3 or IP layer) of the networking protocol framework. (Remarks, pg. 8)

...Kent does disclose or suggest fragmentation avoidance above the IP layer at upper level protocol layers, but it discloses the very opposite, that fragmentation should be performed at the IP datagram layer, i.e., the network layer (i.e., layer 3 or IP layer) of the networking protocol framework.

In response, the examiner finds the arguments of the applicant's representative to be unpersuasive and a mischaracterization of the prior art. Kent does in fact discloses fragmentation at upper protocol levels (applicant's representative is respectfully encouraged to review the reference of Kent and the rejection of claim 1).

Furthermore, the examiner points out that the reference of Kent discloses principles of packet fragmentation and fragmentation avoidance and the reference of IPSEC discloses packet fragmentation avoidance via packet fragmentation of IKE packets above the IP layer (above the UDP layer). In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the examiner respectfully asserts that not only is motivation found within logical reasoning by those of ordinary skill in the art (i.e. rational thought dictates that a teaching to fragment packets would encourage one to make practical application of this teaching), but also within the prior art references (i.e. IPSEC discloses to fragment at an upper level layer and Kent discloses that fragmentation avoidance principles are applicable in an upper level layer).

(ii) *Accordingly, even if IPSEC and Kent were combined, the combination would not disclose or suggest a method for transmitting IKE data packets across a network comprising, inter alia, fragmenting the IKE packet into a plurality of smaller data packets when a response is not received.* (Remarks, pg. 9)

In response, the examiner respectfully encourages the applicant's representative to review the rejection of claim 1, wherein the examiner shows that the combination of IPSEC and Kent discloses fragmentation when *"a response"* is not received.

(iii) *Neither IPSEC nor Kent disclose or suggest the concept of an IKE data packet.* (Remarks, pg. 11)

In response, the examiner respectfully asserts that the prior art discloses IKE data packets (IPSEC, page 4, par. 2; "Revised ESP", pars. 2, 3; page 4, lines 1-8). Herein the context of IPSEC discloses the fragmentation of IKE messages [i.e. packets bearing the certificate payload]. Furthermore, IPSEC discloses that additional problems resulted from the improper utilization by devices of the IKE cookie states (data found within the headers of IKE packets – applicant's representative may refer to the applicant's submitted prior art " (Harkins et al., "The Internet Key Exchange Protocol").

In addition to the above, the examiner respectfully encourages the applicant's representative to review the admission of the applicant's themselves regarding the disclosure of the prior art – namely that IPSEC in fact does disclose or suggest IKE data packets [Remarks, pg. 8 – emphasis added]:

"IPsec deals with a variety of issues relating to the above charter, including ***changes to IKE to support Network Address Translation (NAT)*** *Firewall traversal. (Page 1)*

IPSEC indicates that the testing of IPsec over NAT revealed some problems,

including certificate fragmentation. *(Page 3, last line - page 4, line 6). Possible approaches to avoid fragmentation were considered,* ***including fragmenting packets*** *at a layer of the networking protocol framework that is above the transport layer at which the User Datagram Protocol (UDP) protocol resides. (Page 4, lines 8-10)".*

(iv) *... IPSEC merely discloses that fragmentation of a data packet may occur at a layer above the transport layer of a networking protocol framework, but provides no description of how this fragmentation occurs.*

Nor does Kent disclose the concept of an IKE data packet. (Remarks, pg. 11)

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(v) *As discussed in previous sections, neither PSEC nor Kent disclose or suggest the concept of an IKE packet, nor generating one, attempting whether it was successfully received, or fragmenting one into smaller packets.* (Remarks, pg. 13)

In response, the examiner presumes the applicant's representative to mean "*determining* whether it was successfully received", as "*attempting* whether it was successfully received" does not resemble any claim limitation.

In addition, the examiner respectfully encourages the applicant's representative to review the above claim rejections, responses to arguments, and the prior art, as the concept of an IKE packet, generation of one, determining the successful transmission of a packet, and packet fragmentation are all issues that have been previously discussed.

(vi) *...Kent does not disclose fragmenting any type of packet into a plurality of smaller packets when a response is not received* (Remarks, pg. 14)

In response, the examiner respectfully encourages the applicant's representative to review the above claim rejections (claim 1), responses to arguments (ii), and the prior art, as the concept of fragmentation when *"a response"* is not received has been previously discussed.

(vii) *... IPSEC does not disclose or suggest determining whether fragmentation of a data packet is necessary to successfully transmit IKE information over a network. Accordingly, even if IPSEC and Kent were combined, the resulting combination would not teach or suggest performing the steps of generating, determining and fragmenting independently of performing any steps corresponding to a transport layer protocol and/or a network layer protocol.* (Remarks, pg. 15).

In response to the arguments regarding the limitations added in amendment of claim 18, the examiner respectfully directs the attention of the applicant's representative to the rejection of claim 18.

Furthermore, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *determining whether fragmentation of a data packet is necessary to successfully transmit IKE information over a network*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(viii) Accordingly, even if IPSEC and Kent were combined, the resulting combination would not employ a method of resolving transmitting errors that comprises, inter alia, including an identifier that identifies the data packet in each packet fragment. (Remarks, pg. 17).

In response, the examiner respectfully encourages the applicant's representative to review the above claim rejections, as the concept of including an identifier within a packet has been previously discussed.

(ix) *Thus, Kent does not teach or suggest discarding received packets when a predetermined number of out-of-order packets have been received. PSEC fails to remedy this deficiency of Kent.* (Remarks, pg. 17)

In response, the examiner respectfully encourages the applicant's representative to review the above claim rejections and the prior art. Specifically, Kent discloses receiving a predetermined number [the amount available to buffer] of out of order packets (Kent, section 2.4, par. 3) and Kent discloses discarding at least certain of the received packets (Kent, section 2.4, par. 3). The examiner points out that the section (2.1, par. 3) of Kent was intended to simply show that packets have sequence numbers enabling the system to determine packet ordering. The examiner takes note that the applicant's representative appears to have presumed paragraph 3 of section 2.1 to refer to the second bulleted section of paragraph 1. The examiner had interpreted paragraph 3 as being the paragraph beginning with "Higher level protocols...".

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See Notice of References Cited

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

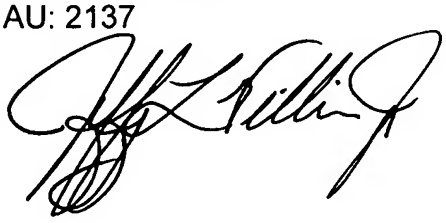
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffery Williams
AU: 2137



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER